

1 **ABSTRACT**

2

3 A method of generating a key by a first correspondent. The key is computable by a second
4 correspondent. The method comprises the steps of:

5 a) making available to the second correspondent a first short term public key;

6 b) obtaining a second short term public key from the second correspondent;

7 c) computing a first exponent derived from the first short term private key, the first short
8 term public key, and the first long term private key;

9 d) computing a second exponent derived from the first short term private key, the first long
10 term public key, the second short term public key and the first long term private key;

11 computing a simultaneous exponentiation of the first exponent with the second short term public
12 key and the second exponent with the second long term public key.